IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA
FORT LAUDERDALE DIVISION

ALEXANDER W. NUNN, on behalf of himself and all others similarly situated, Plaintiff, vs. CITRIX SYSTEMS, INC. and COMCAST CABLE COMMUNICATIONS, LLC, Defendants.	Case No._____ Jury Trial Demanded

CLASS ACTION COMPLAINT

Plaintiff Alexander W. Nunn ("Plaintiff") brings this class action against Defendants Citrix Systems, Inc. ("Citrix") and Comcast Cable Communications, LLC d/b/a Xfinity ("Comcast") (collectively, "Defendants") as an individual and on behalf of all others similarly situated, and alleges as follows upon information and belief:

SUMMARY OF THE CASE

1. This class action arises out of the recent cyberattack and data breach ("Data Breach") resulting from Defendants' failure to implement reasonable and industry standard data security practices.

2. Citrix is a Florida-based software corporation that provides software products and services to its clients that allow those clients to seamlessly manage and monitor their internal applications, including those that allow access to confidential consumer information.

3. Comcast is a limited liability company that provides "broadband, mobile, and

entertainment" products and services to its customers.[1]

4. Plaintiff brings this Complaint against Defendants for their failure to properly secure and safeguard the sensitive information that they collected and maintained as part of their regular business practices, including, but not limited to: names, usernames, password information, contact information, dates of birth, secret questions and answers, and Social Security numbers ("personally identifying information" or "PII").

5. According to CBS News, the sensitive information of approximately 30 million customers has been affected.[2]

6. Upon information and belief, former and current Comcast customers are required to entrust Defendants with sensitive, non-public PII, without which Defendants could not perform their regular business activities, in order to obtain products and/or services from Comcast. Defendants retain this information for at least many years and even after the relationship has ended.

7. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

8. According to the October 10, 2023 "Notice of Data Security Incident" notice that Comcast sent to Plaintiff and other impacted Class Members (the "Notice Letter"):

> October 10, 2023, Citrix announced a vulnerability in software used by Xfinity and thousands of other companies worldwide. Citrix issued additional mitigation guidance on October 23, 2023. Xfinity promptly patched and mitigated the Citrix vulnerability within its systems. However, during a routine cybersecurity exercise on October 25, Xfinity discovered suspicious activity and subsequently determined that between October 16 and October 19, 2023, there was unauthorized access to its internal systems that was concluded to be a result of this vulnerability.[3]

[1] https://corporate.comcast.com/company

[2] https://www.cbsnews.com/news/xfinity-hack-customers-usernames-passwords/

[3] https://www.businesswire.com/news/home/20231218979935/en/Notice-To-Customers-of-Data-Security-Incident; January 2, 2024 email from Xfinity support

9. Subsequently, Comcast "conducted an investigation into the nature and scope of the incident[]" and concluded that "there was unauthorized access to some of [Comcast's] internal systems that we concluded was a result of this vulnerability."[4]

10. Defendants failed to adequately protect Plaintiff's and Class Members' PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendants' negligent and/or careless acts and omissions and their utter failure to protect Comcast's customers' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

11. In breaching their duties to properly safeguard Comcast's customers' PII and give customers timely, adequate notice of the Data Breach's occurrence, Defendants' conduct amounts to negligence and/or recklessness and violates federal and state statutes.

12. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendants' inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts at least to negligence and violates federal and state statutes.

13. Defendants disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable

[4] *Id*.

measures and ensure those measures were followed by their IT vendors to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

14. Plaintiff and Class Members have suffered injuries as a result of Defendants' conduct. These injuries include: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

15. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Comcast's customers' PII from a foreseeable and preventable cyber-attack.

16. Plaintiff seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and

stolen as a result of the Data Breach and who remain at risk due to Defendants' inadequate data security practices.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including Plaintiff, is a citizen of a state different from Defendants.

18. This Court has personal jurisdiction over Defendants because Citrix's principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

19. Venue is proper under 18 U.S.C § 1391(b)(1) because Citrix's principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

PARTIES

20. Plaintiff Alexander W. Nunn is a citizen of Tennessee. Plaintiff lives in Donelson, Tennessee. Plaintiff received an email from Comcast on January 2, 2024 regarding the Data Breach.

21. Defendant Citrix is a corporate citizen of Delaware and Florida. It is a corporation organized under the state laws of Delaware with its principal place of business located in Fort Lauderdale, Florida.

22. Defendant Comcast is a corporate citizen of Delaware and Pennsylvania. It is a limited liability company organized under the state laws of Delaware with its principal place of business located in Philadelphia, Pennsylvania.

FACTUAL ALLEGATIONS

A. Defendants' Businesses

23. Citrix is a Florida-based software corporation that provides software to its clients that allows seamless integration of digital applications, including those that allow access to confidential consumer information.

24. Comcast is a limited liability company that provides "broadband, mobile, and entertainment" products and services to its customers.[5]

25. Plaintiff and Class Members are current and former customers at Comcast.

26. The information held by Defendants in their computer systems or those of their vendors at the time of the Data Breach included the unencrypted PII of Plaintiff and Class Members.

27. Upon information and belief, in the course of collecting PII from Comcast's customers, including Plaintiff, Comcast promised to provide confidentiality and adequate security for their data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

28. Indeed, the Privacy Policy posted on Comcast's website provides that: "[w]e follow industry-standard practices to secure the information we collect to prevent the unauthorized access, use, or disclosure of any personal information we collect and maintain. These security practices include technical, administrative, and physical safeguards, which may vary, depending on the type and sensitivity of the information."[6]

29. Plaintiff and the Class Members, as former and current customers of Comcast,

[5] https://corporate.comcast.com/company

[6] https://www.xfinity.com/privacy/policy

relied on these promises and on these sophisticated business entities to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Customers, in general, demand security to safeguard their PII, especially when their Social Security numbers and other sensitive PII is involved.

30. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class Members relied on the sophistication of Defendants to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

31. Defendants had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. Moreover, Comcast had a duty to audit, monitor, and verify the integrity of its IT vendors and affiliates. Defendants have a legal duty to keep Comcast's customers' PII safe and confidential.

32. Defendants had obligations created by FTC Act, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

33. Defendants derived a substantial economic benefit from collecting Plaintiff and Class Members' PII. Without the required submission of PII, Defendants could not perform the services they provide.

34. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' PII from disclosure.

B. The Data Breach

35. On or about January 2, 2024 (and perhaps as early as December 18, 2023), Comcast began sending Plaintiff and other Data Breach victims a Notice of Data Security Incident emails informing them that:

> **What Happened?** On October 10, 2023, one of Xfinity's software providers, Citrix, announced a vulnerability in one of its products used by Xfinity and thousands of other companies worldwide. At the time Citrix made this announcement, it released a patch to fix the vulnerability. Citrix issued additional mitigation guidance on October 23, 2023. We promptly patched and mitigated our systems.
>
> However, we subsequently discovered that prior to mitigation, between October 16 and October 19, 2023, there was unauthorized access to some of our internal systems that we concluded was a result of this vulnerability. We notified federal law enforcement and conducted an investigation into the nature and scope of the incident. On November 16, 2023, it was determined that information was likely acquired.
>
> **What Information Was Involved?** On December 6, 2023, we concluded that the information included usernames and hashed passwords; for some customers, other information was also included, such as names, contact information, last four digits of social security numbers, dates of birth and/or secret questions and answers. However, our data analysis is continuing, and we will provide additional notices as appropriate.[7]

36. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

37. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data

[7] The "Notice Letter"

Breach is severely diminished.

38. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed. Moreover, Comcast failed to exercise due diligence in selecting its IT vendors or deciding with whom it would share sensitive PII.

39. The attacker accessed and acquired files Defendants shared with a third party containing unencrypted PII of Plaintiff and Class Members. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

40. Plaintiff further believes that he and Class Members' PII was subsequently sold on the dark web following the Data Breach, as that is the modus operandi of cybercriminals that commit cyber-attacks of this type.

C. Data Breaches Are Preventable

41. Defendants could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members or by Comcast exercises due diligence in selecting their IT vendors and properly auditing those vendor's security practices.

42. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

43. The unencrypted PII of Class Members may end up for sale to identity thieves on the dark web, if it has not already, or it could simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members.

Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

44. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[8]

45. To prevent and detect cyber-attacks and/or ransomware attacks Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions— with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

[8] How to Protect Your Networks from RANSOMWARE, at 3, *available at:* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[9]

46. To prevent and detect cyber-attacks or ransomware attacks Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates

- Use threat and vulnerability management

- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong,

[9] *Id*. at 3-4.

randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[10]

47. Given that Defendants were storing the PII of Comcast's current and former customers, Defendants could and should have implemented all of the above measures to prevent and detect cyberattacks.

48. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of more than thirty-five million individuals, including that of Plaintiff and Class Members.

D. Defendants Acquire, Collect, And Store Comcast's Customers' PII

49. Defendants acquire, collect, and store a massive amount of PII on Comcast's

[10] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

customers, former customers, and other personnel.

50. As a condition of obtaining products and/or services from Comcast, Defendants require that customers, former customers, and other personnel entrust Defendants with highly sensitive personal information.

51. By obtaining, collecting, and using Plaintiff's and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' PII from disclosure.

52. Defendants could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members.

53. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII and would not have entrusted it to Defendants absent a promise to safeguard that information.

54. Upon information and belief, in the course of collecting PII from customers, including Plaintiff, Comcast promised to provide confidentiality and adequate security for customer data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

55. Indeed, the Privacy Policy posted on Comcast's website provides that: "[w]e follow industry-standard practices to secure the information we collect to prevent the unauthorized access, use, or disclosure of any personal information we collect and maintain. These security practices include technical, administrative, and physical safeguards, which may vary, depending on the type and sensitivity of the information."[11]

56. Plaintiff and the Class Members relied on Defendants to keep their PII confidential

[11] https://www.xfinity.com/privacy/policy

and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

57. Defendants' negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

E. Defendants Knew, or Should Have Known, of the Risk Because Cable and Software companies In Possession of PII Are Particularly Susceptible To Cyber Attacks

58. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting cable and software companies that collect and store PII, like Defendants, preceding the date of the breach.

59. Data breaches, including those perpetrated against cable and software companies that store PII in their systems, have become widespread.

60. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[12]

61. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendants knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals. Indeed, cyber-attacks, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are

[12] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/

"attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[13]

62. Additionally, as companies became more dependent on computer systems to run their business,[14] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things, the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[15]

63. Defendants knew and understood unprotected or exposed PII in the custody of cable and software companies, like Defendants, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access.

64. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

65. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

66. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of

[13] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?

[14] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html

[15] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022

Plaintiff and Class Members.

67. The ramifications of Defendants' failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

68. As a cable company and software company in custody of Comcast's customers' PII, Defendants knew, or should have known, the importance of safeguarding PII entrusted to them by Plaintiff and Class Members, and of the foreseeable consequences if their data security system were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

F. Value Of Personally Identifying Information

69. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[16] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[17]

70. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity

[16] 17 C.F.R. § 248.201 (2013)

[17] *Id.*

credentials.[18] For example, Personal Information can be sold at a price ranging from $40 to $200.[19] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[20]

71. For example, Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[21]

72. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

73. Even then, a new Social Security number may not be effective. According to Julie

---

[18] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark- web-how-much-it-costs/

[19] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your- personal-information-is-selling-for-on-the-dark-web/

[20] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark

[21] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf

Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[22]

74. Moreover, the compromise of an individual's last four digits of a Social Security number is particularly problematic because the last four digits are frequently used by companies to verify identities and access to customer accounts.[23]

75. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security numbers, dates of birth, and names.

76. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[24]

---

[22] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft

[23] "The numbers were given based on the geographic region, which meant that the first numbers would tell you where someone was from. Meanwhile, the middle two digits are random. But nowadays, a lot of companies ask for the last four digits of the SSN, as they probably think that this is less likely for someone to steal identities. When someone wants to steal the identity of a person, they will do whatever it takes to do it. So, only having the last four digits is not going to stop them. They can even use those digits to take your identity away. Because of this, in certain states, there are some limitations regarding how companies can use your SSN. In places like Rhode Island, for instance, you will not be asked for your last four digits." Frank Gogol, *Why are the Last 4 Digits of an SSN Important?* Stilt (Nov. 3, 2023), available at https://www.stilt.com/immigrants/last-4-digits-of-an-ssn/#

[24] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), a*vailable at*:

77. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

78. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[25]

79. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

G. Defendants Fail To Comply With FTC Guidelines

80. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

81. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose

---

https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html

[25] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf

of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[26]

82. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[27]

83. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

84. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

85. These FTC enforcement actions include actions against cable and software companies, like Defendants.

---

[26] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

[27] *Id.*

86. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

87. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices, and Comcast failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

88. Upon information and belief, Defendants were at all times fully aware of their obligations to protect the PII of Comcast's customers, Defendants were also aware of the significant repercussions that would result from their failure to do so. Accordingly, Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

H. Defendants Fail To Comply With Industry Standards

89. As noted above, experts studying cyber security routinely identify cable and software companies in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

90. Several best practices have been identified that a minimum should be implemented by cable and software companies in possession of PII, like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendants

failed to follow these industry best practices, including a failure to implement multi-factor authentication.

91. Other best cybersecurity practices that are standard in the cable and software industries include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendants failed to follow these cybersecurity best practices, including failure to train staff.

92. Upon information and belief, Defendants failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

I. Common Injuries & Damages

93. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is

subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

J. Data Breaches Increase Victims' Risk of Identity Theft

94. The unencrypted PII of Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

95. Unencrypted PII may also fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Simply put, unauthorized individuals can easily access the PII of Plaintiff and Class Members.

96. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

97. Plaintiff's and Class Members' PII is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

98. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[28]

[28] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sept. 18, 2014),

99. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

100. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

101. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like insurance information) of Plaintiff and the other Class Members.

102. Thus, even if certain information (such as insurance information) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

103. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

K. Loss Of Time To Mitigate Risk Of Identity Theft & Fraud

104. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the

---

https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/

reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

105. Thus, due to the actual and imminent risk of identity theft, Comcast, in its Notice Letter, instructs Plaintiff and Class Members to "remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports."[29]

106. Plaintiff and Class Members have spent, and/or will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter.

107. These mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[30]

108. These mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[31]

---

[29] Notice Letter

[30] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[31] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps

109. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

L. Diminution of Value of PII

110. PII is a valuable property right.[32] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

111. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[33]

112. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[34]

113. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[35, 36]

114. Consumers who agree to provide their web browsing history to the Nielsen

---

[32] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf ("GAO Report").

[33] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4

[34] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/

[35] https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[36] https://datacoup.com/

Corporation can receive up to $50.00 a year.[37]

115. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

116. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

117. The fraudulent activity resulting from the Data Breach may not come to light for years.

118. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

119. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' network, amounting to more than thirty-five million individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

120. The injuries to Plaintiff and Class Members were directly and proximately caused

[37] https://digi.me/what-is-digime/

by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

M. Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

121. Given the type of targeted attack in this case, sophisticated criminal activity, and the type of PII involved, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

122. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her PII was used to file unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

123. Consequently, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

124. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from the Data Breach.

N. Loss of Benefit of The Bargain

125. Furthermore, Defendants' poor data security practices deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Comcast for products and/or services, Plaintiff and other reasonable consumers understood and expected that they were, in

part, paying for the service and necessary data security to protect the PII, when in fact, Defendants did not provide the expected data security. Accordingly, Plaintiff and Class Members received products and/or services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Comcast.

CLASS ACTION ALLEGATIONS

126. Plaintiff brings this class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure on behalf of the following "Class."

> All individuals residing in the United States, or alternatively Tennessee, whose PII was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Comcast in December 2023.

127. Excluded from the Class are Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

128. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. According to the breach report submitted to the Office of the Maine Attorney General, at least 35,000,000 Class Members were impacted in the Data Breach.[38] The Class is apparently identifiable within Defendants' records, and Defendants have already identified these individuals (as evidenced by Comcast sending them breach notification emails).

[38] https://apps.web.maine.gov/online/aeviewer/ME/40/49e711c6-e27c-4340-867c-9a529ab3ca2c.shtml

129. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

a. Whether and to what extent Defendants had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendants had respective duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendants had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the PII of Plaintiff and Class Members;

e. Whether and when Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendants' wrongful conduct;

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

130. Typicality: Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

131. This class action is also appropriate for certification because Defendants acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenges of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

132. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that she has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages she has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intend to prosecute this action vigorously.

133. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

134. The nature of this action and the nature of laws available to Plaintiff and Class

Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

135. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

136. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

137. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the PII of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

138. Further, Defendants have acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

139. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification

because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants failed to timely notify the Plaintiff and the class of the Data Breach;

b. Whether Defendants owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendants' security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendants failed to take commercially reasonable steps to safeguard consumer PII; and Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CLAIMS FOR RELIEF

COUNT I

Negligence

140. Plaintiff re-alleges and incorporates by reference all of the allegations contained in the preceding paragraphs as if fully set forth herein.

141. Defendants require Comcast's customers, including Plaintiff and Class Members, to submit non-public PII to Defendants in the ordinary course of providing their services.

142. Defendants gathered and stored the PII of Plaintiff and Class Members as part of their businesses of soliciting their services to their customers and clients, which solicitations and services affect commerce.

143. Plaintiff and Class Members entrusted Defendants with their PII with the understanding that Defendants would safeguard their information.

144. Defendants had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

145. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which they could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach. Comcast's duty included a responsibility to exercise due diligence in selecting IT vendors and to audit, monitor, and ensure the integrity of its vendor's systems and practices and to give prompt notice to those affected in the case of a data breach.

146. Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

147. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks adequately protected the PII.

148. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted Defendants with their confidential PII, a necessary part of being customers at Comcast.

149. Defendants' duty to use reasonable care in protecting confidential data arose not

only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential PII.

150. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiff or the Class.

151. Defendants also had a duty to exercise appropriate clearinghouse practices to remove Comcast's former customers' PII they were no longer required to retain pursuant to regulations.

152. Moreover, Defendants had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

153. Defendants had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

154. Defendants breached their duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Allowing unauthorized access to Class Members' PII;

d. Failing to detect in a timely manner that Class Members' PII had been compromised;

e. Failing to remove Comcast's former customers' PII they were no longer

required to retain pursuant to regulations,

f. Failing to audit, monitor, or ensure the integrity of their vendor's data security practices;

g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to secure their stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

155. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

156. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statues were intended to guard against.

157. Defendants' violations of Section 5 of the FTC Act constitutes negligence.

158. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

159. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

160. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the

cable and software industry.

161. Defendants have full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

162. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendants' systems or transmitted through third party systems.

163. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

164. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendants' possession.

165. Defendants were in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

166. Defendants' duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

167. Defendants have admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

168. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and

the Class, the PII of Plaintiff and the Class would not have been compromised.

169. There is a close causal connection between Defendants' failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

170. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

171. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

172. Plaintiff and Class Members are entitled to compensatory and consequential

damages suffered as a result of the Data Breach.

173. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II

Negligence *Per Se*

174. Plaintiff re-alleges and incorporates by reference all of the allegations contained in the preceding paragraphs as if fully set forth herein.

175. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

176. Defendants breached their duties to Plaintiff and Class Members under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

177. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se.*

178. Plaintiff and Class Members are within the class of persons that the FTCA intended to protect and the harm to Plaintiff and Class Members resulting from the Data Breach was the type of harm against which the statutes were intended to prevent.

179. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

180. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known

that by failing to meet their duties, Defendants' breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII.

181. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III

Breach of Implied contract

(Against Defendant Comcast)

182. Plaintiff re-alleges and incorporates by reference all of the allegations contained in the preceding paragraphs as if fully set forth herein. Plaintiff brings this claim against solely against Defendant Comcast.

183. Plaintiff and Class Members were required to provide their PII to Comcast as a condition of receiving products and/or services from Comcast.

184. Plaintiff and the Class entrusted their PII to Comcast. In so doing, Plaintiff and the Class entered into implied contracts with Comcast by which Comcast agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

185. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Comcast's data security practices complied with relevant laws and regulations and were consistent with industry standards.

186. Implicit in the agreement between Plaintiff and Class Members and the Comcast to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide

Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

187. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Comcast, on the other, is demonstrated by their conduct and course of dealing.

188. Comcast solicited, offered, and invited Plaintiff and Class Members to provide their PII as part of Comcast's regular business practices. Plaintiff and Class Members accepted Comcast's offers and provided their PII to Comcast.

189. In accepting the PII of Plaintiff and Class Members, Comcast understood and agreed that it was required to reasonably safeguard the PII from unauthorized access or disclosure.

190. On information and belief, at all relevant times Comcast promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

191. On information and belief, Comcast further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

192. Plaintiff and Class Members paid money to Comcast with the reasonable belief and expectation that Comcast would use part of its earnings to obtain adequate data security. Comcast failed to do so.

193. Plaintiff and Class Members would not have entrusted their PII to Comcast in the absence of the implied contract between them and Comcast to keep their information reasonably secure.

194. Plaintiff and Class Members would not have entrusted their PII to Comcast in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

195. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Comcast.

196. Comcast breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

197. As a direct and proximate result of Comcast's breach of the implied contracts, Plaintiff and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

198. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

199. Plaintiff and Class Members are also entitled to injunctive relief requiring Comcast to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT IV

Breach of Third-Party Beneficiary Contract

(Against Defendant Citrix)

200. Plaintiff re-alleges and incorporates by reference all of the allegations contained in the preceding paragraphs as if fully set forth herein. Plaintiff brings this claim against solely against Defendant Citrix.

201. Upon information and belief, Citrix entered into virtually identical contracts with its clients, including Comcast, to provide software products and/or services, which included data security practices, procedures, and protocols sufficient to safeguard the PII that was to be entrusted to it.

202. Such contracts were made expressly for the benefit of Plaintiff and the Class, as it was their PII that Citrix agreed to receive and protect through its services. Thus, the benefit of collection and protection of the PII belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties, and Plaintiff and Class Members were direct and express beneficiaries of such contracts.

203. Citrix knew that if they were to breach these contracts with its clients, Plaintiff and the Class would be harmed.

204. Citrix breached its contracts with its clients and, as a result, Plaintiff and Class Members were affected by this Data Breach when Citrix failed to use reasonable data security and/or business associate monitoring measures that could have prevented the Data Breach.

205. As foreseen, Plaintiff and the Class were harmed by Citrix's failure to use reasonable data security measures to securely store and protect the files in its care, including but not limited to, the continuous and substantial risk of harm through the loss of their PII.

206. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with costs and attorneys' fees incurred in this action.

COUNT V

Unjust Enrichment

207. Plaintiff re-alleges and incorporates by reference all of the allegations contained in the preceding paragraphs as if fully set forth herein.

208. Plaintiff brings this Count in the alternative to the breach of implied contract count

above.

209. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they paid money to Comcast for products and/or services as well as provided Defendants with their PII. In exchange, Plaintiff and Class Members should have received the services that were the subject of the transaction and had their PII protected with adequate data security.

210. Defendants knew that Plaintiff and Class Members conferred a benefit upon them and have accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendants profited from Plaintiff's retained data and used Plaintiff's and Class Members' PII for business purposes.

211. Defendants failed to secure Plaintiff's and Class Members' PII and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PII provided.

212. Defendants acquired the PII through inequitable record retention as they failed to investigate and/or disclose the inadequate data security practices previously alleged.

213. If Plaintiff and Class Members had known that Defendants would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would have entrusted their PII at Defendants or obtained products and/or services at Comcast.

214. Plaintiff and Class Members have no adequate remedy at law.

215. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

216. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy;

(ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

217. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

218. Plaintiff and Class Members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VI

Violation of the Florida Deceptive and Unfair Trade Practices Act Fla. Stat. §§ 501.201 *et seq.*

(Against Defendant Citrix)

219. Plaintiff re-alleges and incorporates by reference all of the allegations contained in the preceding paragraphs as if fully set forth herein. Plaintiff brings this claim against solely against Defendant Citrix.

220. Citrix engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, Comcast obtained Plaintiff's and Class members' PII through advertising, soliciting, providing, offering, and/or distributing goods and services to its clients, including Comcast, and the Data Breach occurred through the use of the internet, an instrumentality of interstate commerce.

221. As alleged herein this Complaint, Citrix engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including, among other things, the following:

a. failing to implement adequate data security practices to safeguard PII;

b. failing to make only authorized disclosures of Citrix's clients' current and former customers' PII;

c. failing to disclose that their data security practices were inadequate to safeguard PII from theft; and

d. failing to timely and accurately disclose the Data Breach to Plaintiff and Class members.

222. Citrix's actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, Citrix engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to Citrix's clients' current and former customers.

223. In committing the acts alleged above, Citrix engaged in unconscionable, deceptive, and unfair acts and practices acts by omitting, failing to disclose, or inadequately disclosing to Citrix's clients' current and former customers that they did not follow industry best practices for the collection, use, and storage of PII.

224. As a direct and proximate result of Citrix's conduct, Plaintiff and Class members have been harmed and have suffered damages including, but not limited to:

225. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiff and Class members have been damaged and are entitled to

recover an order providing declaratory and injunctive relief and reasonable attorneys' fees and costs, to the extent permitted by law.

a. Also, as a direct result of Citrix's knowing violation of the Florida Unfair and Deceptive Trade Practices Act, Plaintiff and Class members are entitled to injunctive relief, including, but not limited to: Ordering that Citrix implement measures that ensure that the PII of Citrix's clients' current and former customers is appropriately encrypted and safeguarded when stored on Citrix's network or systems;

b. Ordering that Citrix purge, delete, and destroy in a reasonable secure manner PII not necessary for their provision of services;

c. Ordering that Citrix routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

d. Ordering Citrix to meaningfully educate its clients' current and former customers about the threats they face as a result of the accessibility of their PII to third parties, as well as the steps its clients' current and former customers must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and each member of the proposed National Class respectfully request that the Court enter judgment in their favor and for the following specific relief against Defendants as follows:

A. That the Court declare, adjudge, and decree that this action is a proper class action and certify each of the proposed Class and/or any other appropriate Class under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including the appointment of Plaintiff's counsel as Class Counsel;

B. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

C. That the Court enjoin Defendant, ordering it to cease and desist from similar unlawful activities;

D. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PHI/PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

E. For injunctive relief requested by Plaintiff, including but not limited to injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an Order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards and federal, state or local laws;

iii. requiring Defendants to delete and purge Plaintiff's and Class Members' PHI/PII unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PHI/PII;

v. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis;

vi. prohibiting Defendants from maintaining Plaintiff's and Class Members' PHI/PII on a cloud-based database;

vii. requiring Defendants to segment data by creating firewalls and access controls so that, if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

viii. requiring Defendants to conduct regular database scanning and securing checks;

ix. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the

employees' respective responsibilities with handling PHI/PII, as well as protecting the PHI/PII of Plaintiff and Class Members;

x. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs and systems for protecting personal identifying information;

xi. requiring Defendants to implement, maintain, review and revise as necessary a threat management program to monitor Defendants' networks for internal and external threats appropriately, and assess whether monitoring tools are properly configured, tested and updated;

xii. requiring Defendants to meaningfully educate all Class Members about the threats they face as a result of the loss of their confidential PHI/PII to third parties, as well as the steps affected individuals must take to protect themselves.

F. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

G. For an award of attorney's fees, costs, and litigation expenses, as allowed by law;

H. For all other Orders, findings and determinations identified and sought in this Complaint.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all claims so triable.

Dated: January 5, 2024.

Respectfully submitted,

/s/ Alexandra C. Warren
Alexandra Warren (FL Bar No. 123960)
Charles J. LaDuca
Brendan Thompson
CUNEO GILBERT & LADUCA, LLP
4725 Wisconsin Avenue NW
Suite 200
Washington, DC 20016
(202) 789-3960
awarren@cuneolaw.com
charles@cuneolaw.com
brendant@cuneolaw.com

Charles Barrett
Daniella Bhadare-Valente
Morgan L. Burkett
NEAL & HARWELL, PLC
1201 Demonbreun St.
Suite 1000
Nashville, TN 37203
(615) 244-1713
cbarrett@nealharwell.com
dbhadare-valente@nealharwell.com
mburkett@nealharwell.com

Attorneys for Plaintiff